Notice of Allowability	Application No.	Applicant(s)	
	10/528,075	WATANABE ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment submitted on 4 March 2009*.

2. ☒ The allowed claim(s) is/are *1-24*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 3/17/05, 2/27/09
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *6/2/09* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Sarah Su/ Examiner, Art Unit 2431	

NOTICE OF ALLOWANCE

1. Amendment B, received on 4 March 2009, has been entered into record. In this amendment, claims 1, 5, 9, 13, and 17 have been amended.

2. Claims 1-24 are presented for examination.

Response to Arguments

3. With regards to the objection to claim 13, the applicant has submitted claim amendments, and the examiner hereby withdraws the objection.

4. Applicant's arguments with respect to claims 1, 9, and 17 have been fully considered and are persuasive. The rejection of 9 December 2008 has been withdrawn.

Information Disclosure Statement

5. The information disclosure statements (IDS) submitted on 17 March 2005 and 27 February 2009 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Examiner's Amendment

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ali M. Imam on 2 June 2009.

The application has been amended as follows:

In claim 1, line 32: delete "including the amount of information of n-k bits," and insert –,wherein the amount of information remaining is n-k bits,–.

In claim 9, lines 17-18: delete "including the amount of information of n-k bits," and insert –,wherein the amount of information remaining is n-k bits,–.

In claim 17, lines 16-17: delete "including the amount of information of n-k bits," and insert –,wherein the amount of information remaining is n-k bits,–.

Allowable Subject Matter

7. Claims 1-24 are allowed.

8. The following is an examiner's statement of reasons for allowance:

Claim 1 discloses of "a cryptographic key creation step of each of the first communication apparatus and the second communication apparatus discarding a part of pieces of the common information after correction according to public error correction information, creating a cryptographic key using information that has remained after discarding, wherein the amount of information remaining is n-k bits, and setting the cryptographic key as a common key which is shared between first communication apparatus and the second communication apparatus." These features, in combination with the other limitations in the claims, are not anticipated by, nor made obvious over, the prior art of record.

Claim 9 discloses of "a cryptographic key creation unit that discards a part of pieces of the common information after error correction according to public error correction information, creates a cryptographic key using information that has remained after discarding, wherein the amount of information remaining is n-k bits, and sets the cryptographic key as a common key which is shared with the communication apparatus on the reception side." These features, in combination with the other limitations in the claims, are not anticipated by, nor made obvious over, the prior art of record.

Claim 17 discloses of "a cryptographic key creation unit that discards a part of pieces of the common information after error correction according to public error correction information, creates a cryptographic key using information that has remained after discarding, wherein the amount of information remaining is n-k bits, and sets the cryptographic key as a common key which is shared with the communication apparatus on the transmission side." These features, in combination with the other limitations in the claims, are not anticipated by, nor made obvious over, the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Elliott (US Patent 7,457,416 B1) discloses a system and method for a key distribution center for quantum cryptographic key distribution networks.

b. Hirota et al. (US 2002/0048370 A1) discloses a system and method for distributing a key.

c. Maeda et al. (US 2006/0093143 A1) discloses a system and method for generating shared information.

d. Young (US Patent 7,492,904 B2) discloses a system and method for QKD system detector autocalibration based on bit-error rate.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431